WE CLAIM:

1	1. A system for controlling access to a platform, the system comprising:
2	a platform having a software services component and an interface component, the
3	interface component having at least one interface for providing access to the software
4	services component for enabling application domain software to be installed, loaded, and run
5	in the platform; and
6	an access controller for controlling access to the software services component by a
7	requesting application domain software via the at least one interface, the access controller
8	comprising:
9	an interception module for receiving a request from the requesting application
10	domain software to access the software services component; and
11	a decision entity for determining if the request should be granted; and
12	wherein the requesting application domain software is granted access to the software
13	services component via the at least one interface if the request is granted.
. 1	2. The system according to claim 1, wherein the decision entity is a security
2	access manager, the security access manager holding access and permission policies.
1	The system according to claim 2, wherein:
2	the request includes an identification of the requesting application domain software;
3	and

4 the security access manager includes a collection of records of approved requesting 5 application domain software for use in determining if the request should be granted to the 6 requesting application domain software based on the identification. 1 4. The system according to claim 3, wherein: 2 the collection of records comprises an access control collection; 3 the security access manager contains an associated permission collection; and 4 the associated permission collection is used to determine if the request should be 5 granted for a requesting application domain software included in the access control 6 collection. 5. 1 The system according to claim 2, wherein the security access manager 2 comprises a decision cache for maintaining a record of requests by application domain 3 software for determining if a permission decision has previously been granted to the requesting application domain software. 4 1 6. The system according to claim 2, wherein: 2 the security access manager has a record of requesting application domain software; 3 and 4 the security access manager determines if the request should be granted based on an 5 identification stored in the record. 1 7. The system according to claim 2, wherein, if the request is denied, a reject 2 message is sent to the requesting application domain software by the interception module.

1	8. 1	ne system according to claim 2, wherein the application domain software	
2	comprises non-r	native application domain software.	
1	9. 1	The system according to claim 8, wherein the non-native application domain	
2	software compri	ises Java application software.	
1	10. 7	The system according to claim 1, wherein the application domain software	
2	comprises native	e application software.	
1	11. 1	The system according to claim 1, wherein the interface component comprises	
2	a middleware se	ervices layer.	
1	12.	The system according to claim 2, wherein the platform comprises a platform	
2	for a mobile term	minal for a wireless telecommunications system.	
1	13. 7	The system according to claim 1, wherein the decision entity is the	
2	interception mo	dule.	
1	14.	The system according to claim 13, wherein:	
2	the requ	est includes an identification of the requesting application domain software;	
3	and		
4	the inter	ception module includes a collection of records of approved requesting	
5	application dom	ain software for use in determining if the permission request should be	
6	granted to the requesting application domain software based on the identification.		

1	15. The system according to claim 14, wherein the interception module comprises
2	a decision cache for maintaining a record of application-software identifiers grouped by
3	native platform service for determining if a permission decision has previously been granted
4	to the requesting application domain software.
1	16. The system according to claim 13, wherein:
2	the interception module has a record for each platform service of the platform; and
3	the interception module determines if the request should be granted based on an
4	identification stored in the record.
1	17. The system according to claim 13, wherein the application domain software
2	comprises non-native application software.
1	18. The system according to claim 13, wherein the application domain software
2	comprises native application software.
1	19. The system according to claim 1, further comprising:
2	a system access module; and
3	wherein the system access module is adapted to update the interception module with
4	information for use by the interception module to determine whether to grant or deny the
5	request.

- 1 20. The system according to claim 19, wherein updates by the system access
- 2 module occur periodically.
- 1 21. The system according to claim 19, wherein updates by the system access
- 2 module occur in response to an update request.

1	22. A method of controlling access to a platform having a software services	
2	component and an interface component, the interface component having at least one interface	
3	for providing access to the software services component for enabling application domain	
4	software to be installed, loaded, and run on the platform, the method comprising:	
5	receiving a request from a requesting application domain software to access the	
6	software services component;	
7	determining if the request should be granted; and	
8	if the request is granted, granting access to the requested software services component	
9	via the at least one interface.	
1	23. The method according to claim 22, wherein:	
2	the request includes an identification of the requesting application domain software;	
3	and	
4	a collection of possible requesting application domain software is used in the step of	
5	determining if the request should be granted.	
1	24. The method according to claim 23, wherein the collection comprises:	
2	an access control collection; and	
3	wherein the determining step comprises accessing the access control collection.	
1	25. The method according to claim 22, wherein the determining step comprises	
2	determining if a decision has previously been granted to the requesting application domain	
3	software.	

2	a record is stored for each platform service of the platform; and
3	the determining step includes determining if the request should be granted to the
4	requesting application domain software based on an identification stored in the record.
1	27. The method according to claim 22, comprising:
2	if the request is denied, sending a reject message to the requesting application domain
3	software.
1	28. The method according to claim 22, wherein the application domain software
2	comprises non-native application software.
1	29. The method according to claim 28, wherein the non-native application domain
2	software comprises Java application software.
1	30. The method according to claim 22, wherein the application domain software
2	comprises native application software.
1	The method according to claim 22, wherein the platform comprises a platform
2	for a mobile terminal for a wireless telecommunications system.
1	32. The method according to claim 22, further comprising updating information
2	used to determine whether to grant or deny the request.

The method according to claim 22, wherein:

1

26.

- 1 33. The method according to claim 32, wherein the step of updating is periodically
- 2 repeated.
- 1 34. The method according to claim 32, wherein the step of updating occurs in
- 2 response to an update request.

2	wireless telecommunications system, the system comprising:
3	a platform having a software services component and an interface component, the
4	interface component having at least one interface for providing access to the software
5	services component for enabling non-native application software to be installed, loaded, and
6	run on the platform; and
7	an access controller for controlling access to the software services component by the
8	non-native application software via the at least one interface, the access controller including:
9	an interception module for receiving a request from the non-native application
10	software to access the software services component; and
11	a decision entity for determining if the request should be granted; and
12	wherein the non-native application software is granted access to the software services
13	component via the at least one interface if the request is granted.
1	36. The system of claim 35, wherein the decision entity is the interception module.
1	37. The system of claim 35, wherein the decision entity is a security access
2	manager.
1	38. The system according to claim 35, wherein the at least one interface comprises
2	a middleware services layer.

A system for controlling access to a platform for a mobile terminal for a

1

35.

- 1 39. The system according to claim 35, wherein the non-native application software comprises Java application software.
- 1 40. The system according to claim 35, wherein native application software may be
- 2 loaded, installed, and run on the platform.